541, 510

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 juillet 2004 (15.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/059976 A2

(51) Classification internationale des brevets[7] : H04N 7/167

(21) Numéro de la demande internationale : PCT/FR2003/050202

(22) Date de dépôt international : 22 décembre 2003 (22.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02 16650 24 décembre 2002 (24.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : VIACCESS [FR/FR]; Les Collines de l'Arche, Tour Opéra C, F-92057 PARIS LA DEFENSE CEDEX (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : MERLE, Gilles [FR/FR]; 41 rue du Hameau, F-78480 VERNEUIL SUR SEINE (FR). BANGUI, François [FR/FR]; 69 rue Dunois, F-75646 PARIS 13ème (FR).

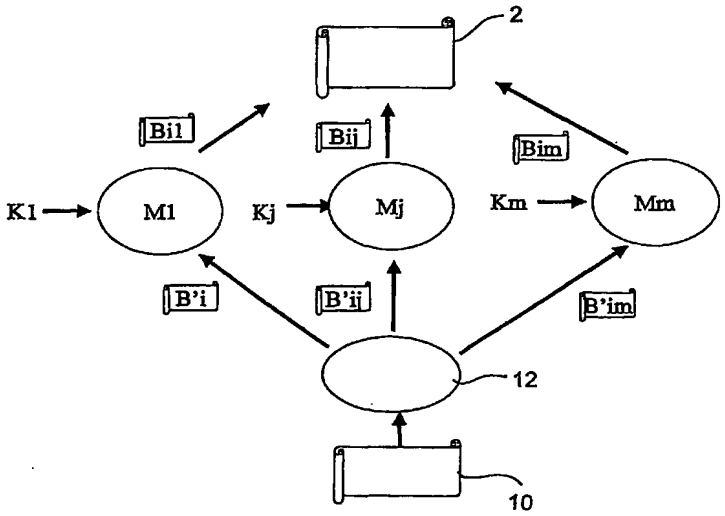
(74) Mandataire : POULIN, Gérard; c/o BREVALEX, 3 rue du Docteur Lancereaux, F-75008 PARIS (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR SECURING SCRAMBLED DATA

(54) Titre : PROCEDE ET SYSTEME DE SECURISATION DE DONNEES EMBROUILLEES



(57) Abstract: The invention relates to a controlled-access method of distributing scrambled data to at least one receiving terminal. The inventive method involves a first encryption phase comprising the following steps consisting in: subdividing the data into a whole number of families Fj (j=1...M) each containing a whole number of blocks Bi (i=1...N); allocating a specific identification parameter pj (j=1...M) to each family Fj, said parameter being associated with at least one descrambling module Mj having a specific processing capacity and a specific security level; scrambling each block Bi of a family Fj of type pj with a key Kj (j=1...M) in a one-to-one relationship with parameter pj. The invention also involves a second descrambling phase comprising the following steps consisting in: identifying the family of each block Bi and descrambling each block Bi of a family of type pj with module Mj using key Kj.

[Suite sur la page suivante]

WO 2004/059976 A2

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de distribution avec contrôle d'accès de données embrouillées à moins un terminal récepteur. Le procédé selon l'invention comporte - une première phase de chiffrement comprenant les au étapes suivantes • subdiviser lesdites données en un nombre familles Fj (j=l...M) comportant chacune un nombre entier de blocs Bi (i=l ...N) , • affecter à chaque famille Fj un paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques, • embrouiller chaque bloc Bi d'une famille Fj de type pj par une clé Kj (j=1...M) en relation biunivoque avec le paramètre pj, une deuxième phase de désembrouillage comportant entier de - et les étapes suivantes • identifier la famille de chaque bloc Bi, • désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj au moyen de la clé Kj.

PROCEDE ET SYSTEME DE SECURISATION DE DONNEES EMBROUILLEES

DOMAINE TECHNIQUE

L'invention se situe dans le domaine du contrôle d'accès à des données embrouillées.

Elle concerne plus spécifiquement un procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs, chacun desdits terminaux étant muni d'une pluralité de modules de désembrouillage Mj (j=1...M) ayant chacun une capacité de traitement et un niveau de sécurité spécifique, lesdites données étant préalablement subdivisées en un nombre entier de familles Fj (j=1...M) comportant chacune un nombre entier de blocs Bi (i=1...N), chaque bloc Bi (i=1...N) d'une famille Fj étant embrouillés par une clé Kj (j=1...M) associée à la famille Fj.

Les terminaux récepteurs sont des équipements mobiles (ME) (pour Mobile Equipment en anglais) à usage grand public tels que par exemple des téléphones portables, des assistants numériques personnels appelés PDA (pour Personal Digital Assistant en anglais) ou encore des récepteurs audiovisuels ou des ordinateurs.

L'invention concerne également un système de sécurisation de données et/ou services comportant une plate-forme d'embrouillage et une plate-forme de désembrouillage destinées à mettre en œuvre le procédé.

Les données à sécuriser sont des œuvres littéraires ou artistiques protégées par un système numérique de gestion de droits DRM (pour Digital Right Management). Ces oeuvres peuvent être soit mémorisées sur un support tel que par exemple un CD ROM ou un DVD,

soit transmises ou téléchargées à partir d'un serveur distant vers une pluralité de terminaux récepteurs connectés à un réseau de transmission.

ETAT DE LA TECHNIQUE ANTERIEURE

Dans les systèmes de sécurisation de données de l'art antérieur, le contenu à protéger (audio, vidéo, texte...) est embrouillé chez l'opérateur et déchiffré lors de sa réception chez l'abonné par un algorithme de désembrouillage mémorisé dans le terminal récepteur.

Un inconvénient majeur de ces systèmes provient du fait qu'à la réception, tout le contenu distribué est désembrouillé par un même module de désembrouillage. Aussi, en cas de piratage, la totalité de ce contenu devient accessible et peut alors être redistribué frauduleusement sur des réseaux illicites.

Une première solution connue pour pallier à ce problème consiste à confiner le module de désembrouillage dans un local à accès sécurisé. Cette solution n'est pas adaptée aux applications dans lesquelles les terminaux sont à usage grand public.

Une deuxième solution, basée sur le renforcement de la sécurité du récepteur lui-même, consiste à empêcher l'installation sur le terminal de tout logiciel suspect et d'autoriser l'installation uniquement de logiciels « certifiés », c'est-à-dire, des logiciels pour lesquels une autorisation de téléchargement a été donnée.

Cette solution n'est pas non plus adaptée aux applications citées ci-dessus qui utilisent des récepteurs « ouverts » munis d'une interface d'entrée

sortie permettant de télécharger tout type de logiciels (ordinateurs, récepteurs audio et vidéo) par opposition aux terminaux « verrouillés » par fabrication, tels que les décodeurs par exemple, pour empêcher un abonné de télécharger frauduleusement des logiciels de désembrouillage.

Le but de l'invention est de pallier les inconvénients de l'art antérieur cités ci-dessus.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs dans lequel chacun desdits terminaux est muni d'une pluralité de modules de désembrouillage Mj (j=1…M) ayant chacun une capacité de traitement et un niveau de sécurité spécifique, et dans lequel les données sont préalablement subdivisées en un nombre entier de familles Fj (j=1…M) comportant chacune un nombre entier de blocs Bi (i=1…N), chaque bloc Bi (i=1…N) d'une famille Fj étant ensuite embrouillés par une clé Kj (j=1…M) associée à la famille Fj.

Selon l'invention lesdits bloc Bi (i=1…N) sont préalablement organisés en fonction des vitesses respectives de traitement des modules de désembrouillage Mj.

Selon l'invention, les modules Mj (j=1…M) sont des éléments périphériques différents associés audit terminal récepteur.

Grâce à l'invention, une attaque sur l'un des modules Mj (j=1…M) permet de reconstruire un fichier

qui n'est pas complet car il manque la partie traitée par les autres modules. Le fichier piraté sera fortement dégradé par rapport à l'original et donc inexploitable.

Dans un premier mode de réalisation, les modules de désembrouillage Mj (j=1...M) comportent des algorithmes Aj (j=1...M) différents.

Dans un deuxième mode de réalisation les modules de désembrouillage Mj (j=1...M) comportent des algorithmes Aj (j=1...M) identiques.

Dans les deux modes de réalisation, les données à distribuer se présentent sous forme d'un fichier préalablement mémorisé ou sous forme d'un flux diffusé en temps réel.

Dans une application particulière du procédé selon l'invention, le flux de données représente des programmes audio et/ou vidéo ou des dessins animés (animation multimédia), ou encore des images de synthèses protégées par un système DRM.

L'invention concerne également un système de sécurisation de données embrouillées comportant une plate-forme d'embrouillage et une plate-forme de désembrouillage.

La plate-forme d'embrouillage comporte:

- des moyens pour subdiviser ledit flux en m familles distinctes de N blocs Bi (i=1...N),
- des moyens pour affecter à chaque famille un paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques,
- des moyens pour embrouiller chaque bloc Bi par une

clé Kj (j=1...M) en relation biunivoque avec le paramètre pj.

Selon une caractéristique essentielle de l'invention, ladite plate-forme de désembrouillage comporte des moyens pour identifier la famille de chaque bloc Bi de manière à désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj correspondant audit paramètre pj.

Selon un mode préféré de réalisation, la plate-forme de désembrouillage comporte une pluralité de modules de désembrouillage distincts Mj (i=1...M).

Dans une variante de réalisation de l'invention, les données à sécuriser sont des programmes audiovisuels diffusés à une pluralité d'abonnés munis de licence d'utilisation gérée par un système DRM.

L'équipement mobile peut être un PDA ou un téléphone mobile muni d'une carte à puce de type SIM (pour Subsciber Identity Module, en anglais).

Dans ce cas, les données sont réparties entre un premier module de désembrouillage M1 intégré dans le PDA (respectivement dans le téléphone mobile) et un deuxième module de désembrouillage M2 constitué par la carte à puce elle-même.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif en référence aux figures annexées dans lesquelles :

- la figure 1 illustre schématiquement une étape de

typage de données à sécuriser par le procédé selon l'invention,

- la figure 2 illustre schématiquement une étape d'embrouillage d'une famille de données obtenue par l'étape précédente,
- la figure 3 illustre schématiquement un premier mode de réalisation de la première et de la deuxième étape du procédé selon l'invention,
- la figure 4 représente schématiquement la phase de désembrouillage des familles de données obtenues par les étapes précédentes,
- la figure 5 représente un mode préféré de réalisation de l'étape illustrée par la figure 4,
- la figure 6 représente schématiquement un terminal mettant en œuvre le procédé selon l'invention,
- la figure 7 représente un diagramme temporel illustrant schématiquement le traitement par le procédé selon l'invention d'un flux de données diffusées ou téléchargé en temps réel par le terminal,
- la figure 8 représente un diagramme temporel illustrant la gestion des clés d'embrouillage du flux de la figure 7.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

La description qui suit concerne une application de l'invention dans laquelle les données embrouillées représentent des programmes audio et/ou vidéo diffusés ou téléchargés vers un PDA (pour Personal Digital Assistant) muni d'une carte à puce de type SIM. Le PDA comporte un premier module M1 de

désembrouillage, un deuxième module de désembrouillage étant la carte SIM elle-même.

Les données à sécuriser peuvent être téléchargées à partir d'un support d'enregistrement (CD, DVD…) ou à partir d'un serveur spécialisé (Musique, vidéo, dessins animés, sonneries téléphoniques, livre électronique E-Book…).
Elles peuvent également être diffusées dans un réseau.

Quels que soient l'application envisagée et le type de données, avant la distribution de ces données, le procédé comporte :

- une première phase de traitement comportant :
  - une étape de typage consistant à former m familles Fj (j= 1…M) de données comportant chacune un nombre nj blocs de données Bi (i=1…N), chaque famille étant identifiée par un paramètre pj.
  - une étape d'embrouillage de chaque bloc Bi d'une famille Fj par une clé Kj (j=1…M) en relation biunivoque avec le paramètre pj.
- et à réception des données par un terminal, celles-ci subissent une deuxième phase de traitement comportant :
  - une étape d'identification de la famille de chaque bloc Bi reçu,
  - une étape de désembrouillage de chaque bloc Bi au moyen de la clé Kj par un module Mj (j=1…M) identifié par un paramètre pj.

Selon une caractéristique essentielle de l'invention, les module Mj (j=1…M) qui permettent de désembrouiller les blocs Bi de deux familles distinctes sont différents.

Ceux-ci peuvent être soit des périphériques différents associés au terminal récepteur, ou des logiciels indépendants stockés dans la mémoire du terminal ou d'un périphérique.

Cas d'un fichier de données préalablement mémorisé.

Typage

La figure 1 représente un fichier 2 de données audio et/ou vidéo organisées en blocs appelés unités d'accès AU (pour Access Unit) selon la norme MPEG 4 (pour Motion Picture Expert Group).

Une première étape 4 du procédé consiste à découper le fichier 2 en m familles Fj (j=1...m) comportant chacune un nombre entier nj de blocs Bi (i=1...N); Chaque famille Fj est identifiée par paramètre pj (j=1...m).

Le paramètre p_j identifie également le module Mj qui sera chargé de désembrouiller les blocs Bi de la famille Fj.

Dans l'application décrite, le fichier est découpé en deux familles F_1 et F_2 dont les blocs respectifs seront désembrouillés respectivement par un module M1 intégré au PDA et par la carte SIM constituant le module M2.

Lors du typage, un paramètre p1 est associé à la famille F1 de blocs Bi qui seront désembrouillés par le module M1 et un paramètre p2 est associé à la famille F_2 de blocs B_i qui seront désembrouillés par la carte SIM.

Embrouillage

La figure 2 illustre une deuxième étape 6 au cours de laquelle les blocs Bi d'une famille F_j sont embrouillés par une clé K_j (j=1,2) définie en fonction de la capacité de traitement et du degré de sécurité respectifs du module M_1 intégré au PDA et de la carte SIM. Les blocs embrouillées B'_i sont stockés dans un fichier 8.

Dans une variante de réalisation du procédé illustrée schématiquement par la figure 3, le typage 4 et l'embrouillage 6 d'un bloc B_i sont réalisés successivement.

Dans une autre variante de réalisation non représentée, l'embrouillage est réalisé famille par famille.

Le fichier 10 contenant les blocs B'_i embrouillés est ensuite transmis au PDA.

Désembrouillage

La figure 4 illustre la phase de désembrouillage d'un fichier 10 comportant des familles Fj distinctes de blocs MPEG préalablement embrouillés.

A l'étape 12, les blocs B'_i sont identifiés par leur paramètre respectif p_j puis aiguillés sur les modules de désembrouillage correspondant M_j.

Les blocs déchiffrés sont ensuite réarrangés pour former le fichier d'origine 2 qui sera fourni à l'utilisateur.

La figure 5 illustre schématiquement un mode préféré de réalisation du désembrouillage dans lequel les blocs Bi contenus dans le fichier 10 sont traités à

la volée bloc par bloc.

Traitement temporel d'un flux de données

La figure 6 représente schématiquement les modules internes d'un PDA permettant de réaliser le désembrouillage.

Le PDA illustré comporte un étage d'entrée 20 chargé d'identifier les blocs B'i dans un flux, un étage 22 de démultiplexage, un premier module de désembrouillage 24, une carte à puce constituant un deuxième module de désembrouillage 26, un étage de multiplexage 28 et un étage de sortie 30.

La figure 7a illustre schématiquement un flux de données diffusé ou téléchargé comportant des blocs Bi au format MPEG 4.

Un premier traitement de ce flux, réalisé au niveau de l'émetteur, consiste à réorganiser les blocs MPEG en fonction des capacités et des vitesses respectives de traitement du module M1 et de la carte SIM.

La figure 7b représente le flux de la figure 7a dans laquelle ont été créées une famille formée par des blocs de type A et une famille formée par des blocs de type B.

Dans cet exemple, les blocs de type A seront désembrouillés par le module M1 et les blocs de type B par la carte SIM.

Du fait que la capacité et la vitesse de traitement de la carte SIM sont inférieures à celles du décodeur, à l'émission, les blocs de type B sont

décalés de trois blocs en amont de manière à compenser la différence de vitesse de traitement entre le décodeur et la carte SIM.

La figure 7c représente la répartition temporelle des blocs du flux diffusé après embrouillage et réorganisation.

La figure 7d représente la répartition temporelle des blocs du flux reçus par le PDA avant désembrouillage, et la figure 7e représente la répartition temporelle des blocs du flux désembrouillé.

La figure 8 illustre schématiquement le mécanisme de changement de clés pour désembrouiller les blocs du flux traité.

On désigne par crypto-période la durée de validité d'une clé de désembrouillage. Avant chaque début de crypto-période un message est inséré dans le flux afin de prévenir le module de désembrouillage du changement de crypto-période. Ce message contient l'ensemble des informations nécessaires pour désembrouiller le flux pendant la crypto-période suivante (par exemple la référence de la clé de désembrouillage à utiliser). Ce message est inséré dans le flux avant le début de la crypto-période (delay start) afin de permettre au module de désembrouillage de traiter les informations du message et d'être prêt à désembrouiller en temps réel les données de la crypto-période à venir.

Les Applications

Cette invention s'applique à des contenus où la perte d'une partie de l'information rend le contenu inexploitable. Cela s'applique à l'ensemble des

contenus audio et vidéo numériques compressés où la perte d'information se traduit par une dégradation rapide de la qualité (audio, vidéo, Ebook, sonneries de téléphones portable, image..).

Les modules de déchiffrement visés sont :

- des supports amovibles type carte à puce, carte à puce sans contact, module détachable (PCMCIA, série, USB, Ethernet).
- des terminaux type PC, serveur, décodeur numérique, récepteur mobile (Téléphone Mobile, PDA).

Les services :

- VOD (Video On Demand) en diffusion ou en téléchargement,
- MOD (Music On Demand) en diffusion ou en téléchargement,
- Diffusion de livre électronique en ligne,
- Diffusion de sonnerie pour téléphone mobile,
- Diffusion de photo/image,
- Diffusion de texte, document multimédia.

REVENDICATIONS

1. Procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs, chacun desdits terminaux étant muni d'une pluralité de modules de désembrouillage Mj (j=1…M) ayant chacun une capacité de traitement et un niveau de sécurité spécifique, lesdites données étant préalablement subdivisées en un nombre entier de familles Fj (j=1…M) comportant chacune un nombre entier de blocs Bi (i=1…N), chaque bloc Bi (i=1…N) d'une famille Fj étant embrouillés par une clé Kj (j=1…M) associée à la famille Fj, procédé caractérisé en ce que lesdits bloc Bi (i=1…N) sont préalablement organisés en fonction des vitesses respectives de traitement des modules de désembrouillage Mj.

2. Procédé selon la revendication 1, caractérisé en ce que les modules Mj (j=1…M) sont des éléments périphériques différents associés audit terminal récepteur.

3. Procédé selon la revendication 2, caractérisé en ce que les modules de désembrouillage Mj (j=1…M) comportent des algorithmes Aj (j=1…M) différents.

4. Procédé selon la revendication 2, caractérisé en ce que les module de désembrouillage Mj (j=1…M) comportent des algorithmes Aj (j=1…M) identiques.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à distribuer se présentent sous forme d'un fichier préalablement mémorisé.

6. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à sécuriser se présentent sous forme d'un flux diffusé ou téléchargé et traité en temps réel par le terminal.

7. Procédé selon les revendications 5 ou 6, caractérisé en ce que la durée d'utilisation du flux est divisée en crypto-périodes correspondant chacune à une clé de désembrouillage, et en ce qu'avant chaque début de crypto-période un message est inséré dans le flux afin de prévenir le module de désembrouillage Mj du changement de crypto-période.

8. Procédé selon la revendication 7, caractérisé en ce que ledit message comporte l'ensemble des informations nécessaires pour désembrouiller le flux utilisé pendant la crypto-période suivante.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent des programmes audio et/ou vidéo protégés par un système DRM.

10. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent des images de synthèse ou des dessins animés.

11. Système de sécurisation de données embrouillées fournies à au moins un terminal récepteur, caractérisé en ce qu'il comporte :

- une plate-forme d'embrouillage comprenant :
  - des moyens pour subdiviser lesdites données en m familles distinctes de N blocs Bi (i=1…N),
  - des moyens pour affecter à chaque famille Fj un paramètre spécifique d'identification pj (j=1…M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques,
  - des moyens pour embrouiller chaque bloc Bi par une clé Kj (j=1…M) en relation biunivoque avec le paramètre pj,
- et une plate-forme de désembrouillage comportant des moyens pour identifier la famille de chaque bloc Bi de manière à désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj correspondant audit paramètre pj.

12. Système selon la revendication 11, caractérisé en ce que les modules de désembrouillages distincts Mj (j=1…M) sont des périphériques distincts associés au terminal récepteur.

13. Plate-forme d'embrouillage d'un flux de données, caractérisée en ce qu'elle comporte :

- des moyens pour subdiviser ledit flux en m familles distinctes de N blocs Bi (i=1…N),
- des moyens pour affecter à chaque famille un

paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques,

- des moyens pour embrouiller chaque bloc Bi par une clé Kj (j=1...M) en relation biunivoque avec le paramètre pj.

14. Plate-forme de désembrouillage d'un flux de données embrouillé par la plate-forme de la revendication 13, caractérisée en ce qu'elle comporte des moyens pour identifier la famille de chaque bloc Bi de manière à désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj correspondant audit paramètre pj.

15. Plate-forme de désembrouillage selon la revendication 14, caractérisée en ce qu'elle comporte une pluralité de modules de désembrouillage distincts Mj (i=1...M) identifiés chacun par le paramètre spécifique d'identification pj.

16. Plate-forme de désembrouillage selon la revendication 15, caractérisée en ce que le terminal récepteur est un PDA et en ce que l'un desdits modules de désembrouillage Mj (i=1...M) est intégré au PDA et au moins deuxième module est une carte à puce de type SIM connectée audit PDA.

17. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de vidéo

à la demande (VOD).

18. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de Musique à la demande (MOD).

19. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser l'accès à un service diffusion de livre électronique en ligne ou téléchargé à partir d'un support amovible.

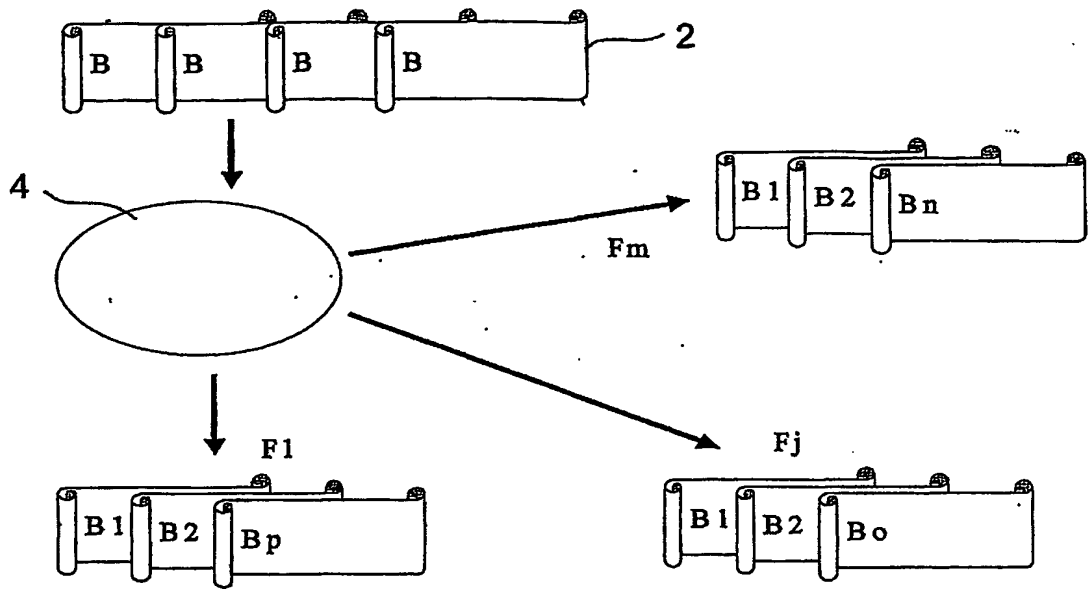

B
B
B
B
2
4
Fm
B1
B2
Bn
F1
B1
B2
Bp
Fj
B1
B2
Bo

FIG. 1

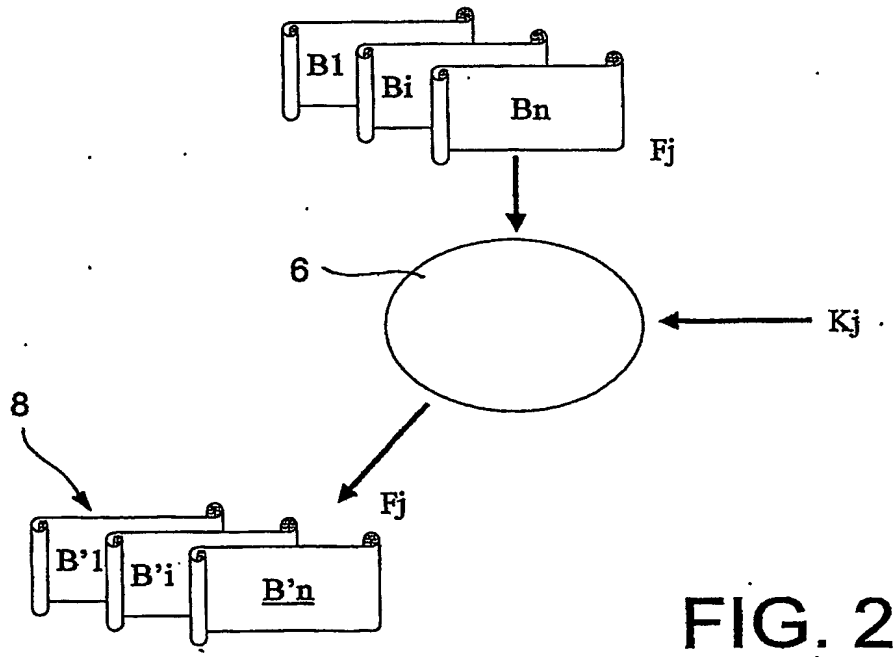

B1
Bi
Bn
Fj
6
Kj
8
Fj
B'1
B'i
B'n

FIG. 2

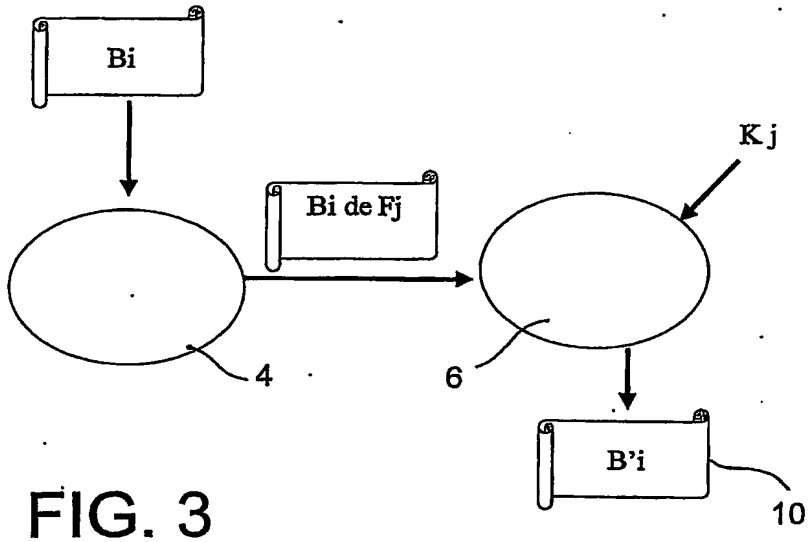

Bi
Bi de Fj
Kj
4
6
B'i
10

FIG. 3

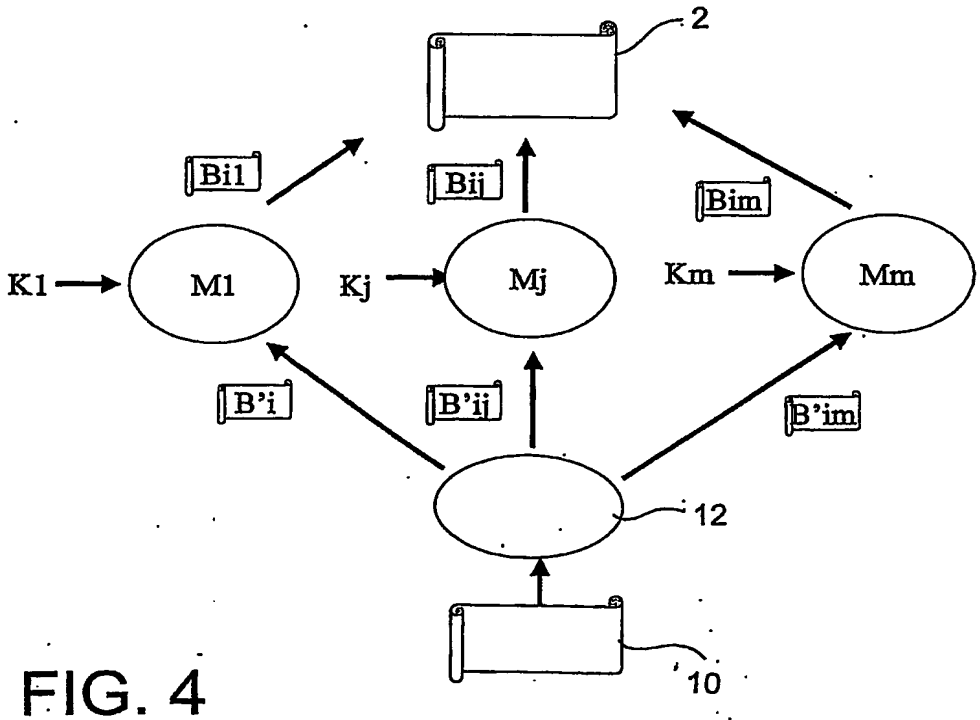

2
Bi1
Bij
Bim
K1
M1
Kj
Mj
Km
Mm
B'i
B'ij
B'im
12
10

FIG. 4

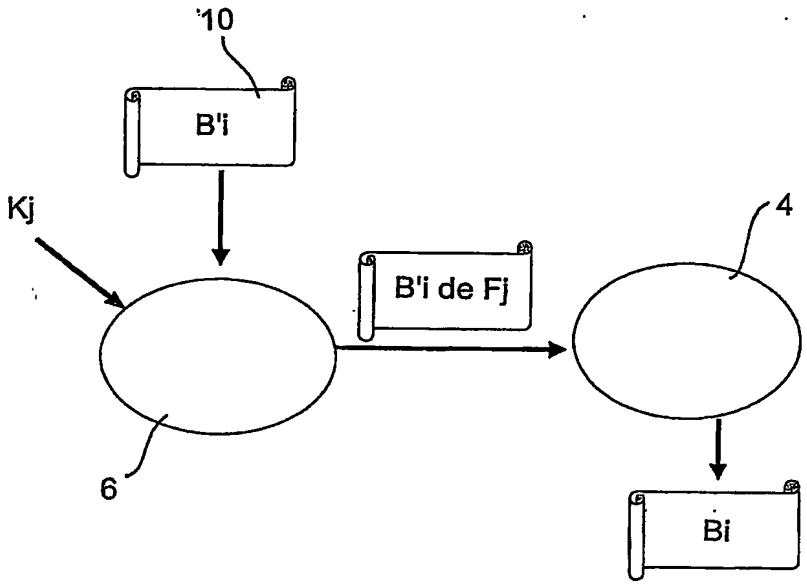


FIG. 5

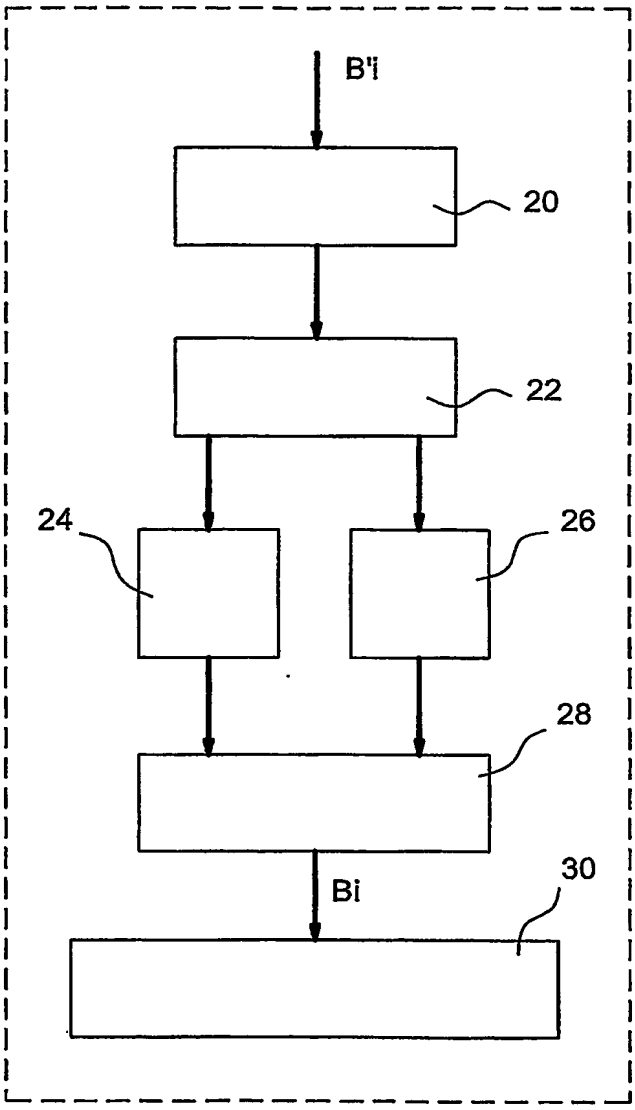
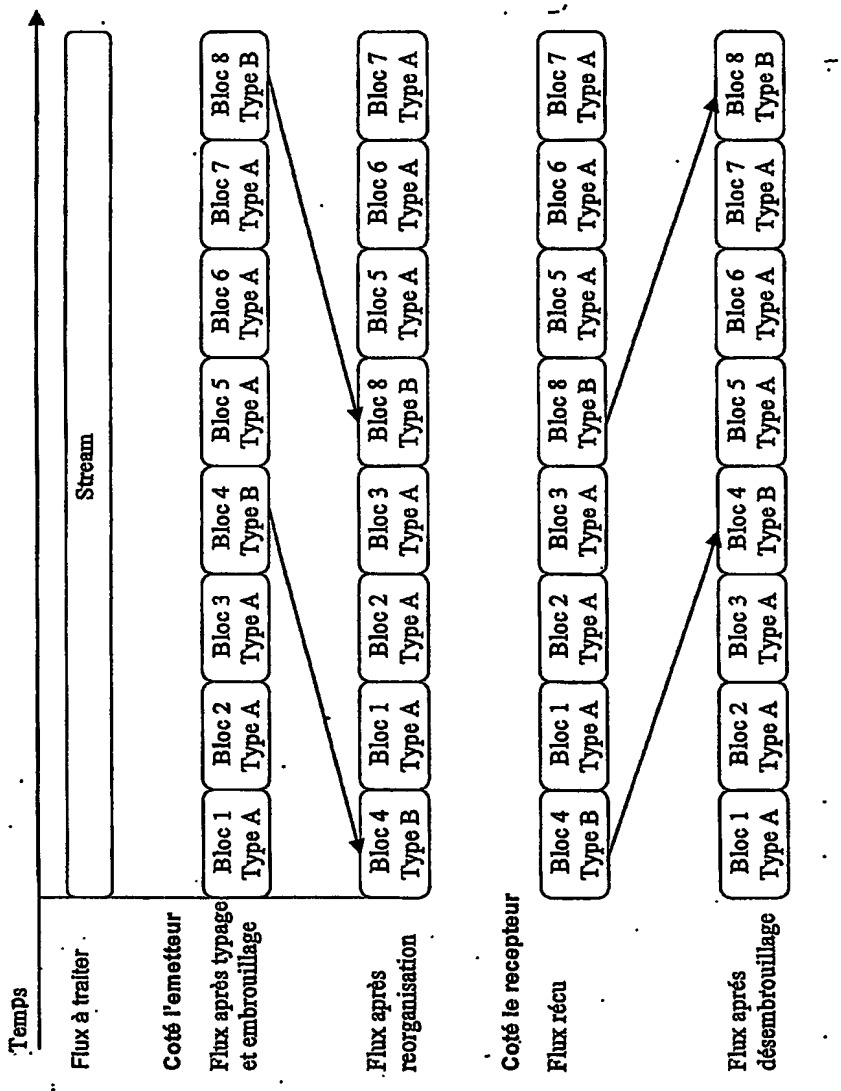


FIG. 6

FIG. 7


a
b
c
d
e
Temps
Flux à traiter
Stream
Coté l'emetteur
Flux après typage et embrouillage
Bloc 1 Type A
Bloc 2 Type A
Bloc 3 Type A
Bloc 4 Type B
Bloc 5 Type A
Bloc 6 Type A
Bloc 7 Type A
Bloc 8 Type B
Flux après reorganisation
Bloc 4 Type B
Bloc 1 Type A
Bloc 2 Type A
Bloc 3 Type A
Bloc 8 Type B
Bloc 5 Type A
Bloc 6 Type A
Bloc 7 Type A
Coté le recepteur
Flux récu
Bloc 4 Type B
Bloc 1 Type A
Bloc 2 Type A
Bloc 3 Type A
Bloc 8 Type B
Bloc 5 Type A
Bloc 6 Type A
Bloc 7 Type A
Flux aprés désembrouillage
Bloc 1 Type A
Bloc 2 Type A
Bloc 3 Type A
Bloc 4 Type B
Bloc 5 Type A
Bloc 6 Type A
Bloc 7 Type A
Bloc 8 Type B

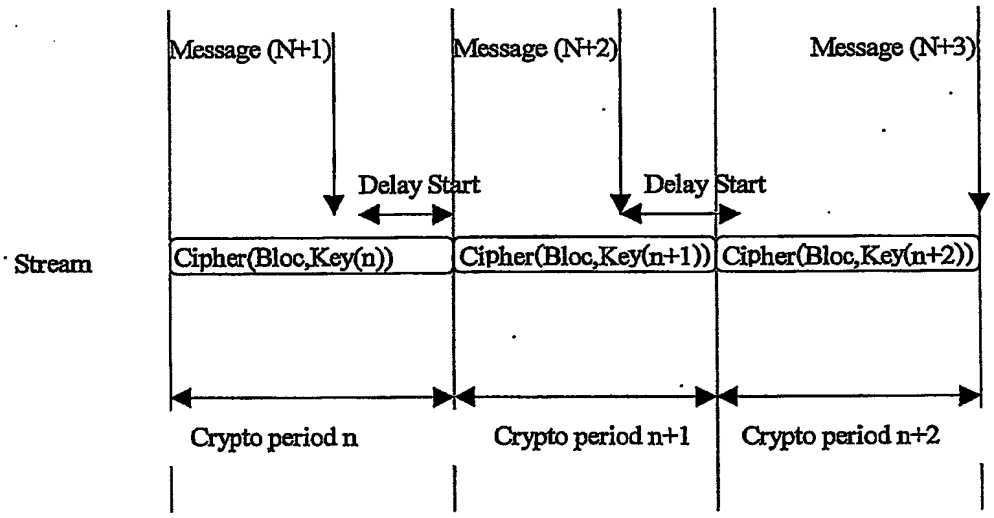

Message (N+1)
Message (N+2)
Message (N+3)
Delay Start
Delay Start
Stream
Cipher(Bloc,Key(n))
Cipher(Bloc,Key(n+1))
Cipher(Bloc,Key(n+2))
Crypto period n
Crypto period n+1
Crypto period n+2

FIG. 8